IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A post issuance system for performing data or configuration changes within a personal security device (PSD), said system comprising:

said PSD, including at least one functional application and a PSD cryptographic component,

a local client functionally connected to said PSD,

a first server functionally connected to said local client, said ~~PSD~~ client and said first server comprising a first component for mutual authentication,

at least one hardware security module (HSM), including an HSM cryptographic component complementary to said PSD cryptographic component, said at least one HSM being functionally connected to said first server,

a communications pipe, established between said PSD and said at least one HSM, and

~~a~~ at least one storage component that stores or generates said data or configuration changes, said at least one storage component being functionally connected to said first server, wherein:

said at least one HSM comprises a controlling component that controls said data or configuration changes sent through said communications pipe to said PSD, after said client and said first server are mutually authenticated.

2. (Previously Presented) The system according to claim 1 comprising a network for the establishment of said communications pipe.

3. (Previously Presented) The system according to claim 1 wherein said at least one functional application includes a component that processes APDU commands and said data or configuration changes received through said communications pipe.

4. (Currently Amended) The system according to claim 1 further comprising:

at least one second server in processing communications with said first server, wherein:

said at least one second server includes or generates stored data or configuration changes retrievable using a PSD unique identifier.

5. (Previously Presented) The system according to claim 4 wherein said first server and said at least one second server comprise a component for mutual authentication.

6. (Previously Presented) The system according to claim 1 wherein said at least one functional application includes an application identifier.

7. (Previously Presented) The system according to claim 6 comprising a selecting component that selects said at least one functional application using said application identifier.

8. (Previously Presented) The system according to claim 4 further comprising:

a network for the establishment of said communications pipe and for functionally connecting said at least one second server to said first server, and

a sending component that sends said retrieved data or configuration changes from said at least one second server over said network to said first server.

9. (Previously Presented) The system according to claim 4 wherein:

said first server comprises a first processing component that receives and processes said data or configuration changes, and

said at least one HSM comprises a second processing component that further processes said data or configuration changes.

10. (Previously Presented) The system according to claim 1 wherein said at least one HSM comprises a generating component that generates at least one command executable by said at least one functional application.

11. (Currently Amended) The system according to claim 1 ~~10~~ wherein said at least one HSM comprises an encrypting component that encrypts ~~said~~ at least one command executable by said at least one functional application ~~and~~ or said data or configuration changes, forming at least one cryptogram.

12. (Previously Presented) The system according to claim 11 further comprising a sending component that sends said at least one cryptogram through said communications pipe into said PSD for processing by said at least one functional application.

13. (Previously Presented) The system according to claim 12 wherein said at least one functional application comprises:

a decrypting component that decrypts said cryptogram using said PSD cryptographic component, and

an executing component that executes said at least one command.

14. (Previously Presented) The system according to claim 2 wherein said network is a public network.

15. (Previously Presented) The system according to claim 2 wherein said network is a private network.

16. (Original) The system according to claim 1 wherein said communications pipe is provided with a secure communications protocol.

17. (Previously Presented) The system according to claim 1 wherein said HSM cryptographic component and said PSD cryptographic component comprise complementary asymmetric keys.

18. (Currently Amended) The system according to claim 1 wherein said HSM cryptographic component and said PSD

cryptographic component ~~comprise~~ store or are able to generate complementary symmetric keys.

19. (Currently Amended) A post issuance method for performing data or configuration changes within a personal security device (PSD), said method comprising:

establishing a communications pipe between said PSD and at least one hardware security module (HSM), wherein said PSD is functionally connected to a local client and said at least one HSM is functionally connected to a first server,

mutually authenticating said ~~PSD~~ client and said first server,

selecting, after mutually authenticating said client and said first server, at least one functional application within said PSD associated with existing data or configurations,

generating or retrieving cryptographic key material from an HSM cryptographic component complementary to a cryptographic component included inside said PSD,

retrieving said data or configuration changes,

processing said data or configuration changes by said first server,

encrypting said processed data or configuration changes by said at least one HSM using said complementary HSM cryptographic component,

routing said encrypted processed data or configuration changes through said communications pipe into said PSD, and

decrypting and processing said processed data or configuration changes by said at least one functional application using said PSD cryptographic component.

20. (Previously Presented) The method according to claim 19, further comprising:

retrieving said data or configuration changes from at least one second server, and

sending said data and configuration changes over a network from said second server to said first server.

21. (Previously Presented) The method according to claim 20 further comprising mutually authenticating said at least one second server and said first server.

22. (Currently Amended) The method according to claim 21, further comprising using a unique identifier associated with said

at least one functional application ~~PSD~~ for mutually authenticating said PSD and said first server.

23. (Currently Amended) The method according to claim 19, further comprising using a unique identifier associated with said at least one functional application ~~PSD~~ for selecting said at least one functional application.

24. (Currently Amended) The method according to claim 19, further comprising using a unique identifier associated with said at least one functional application ~~PSD~~ for generating or retrieving said HSM cryptographic key material ~~component~~.

25. (Currently Amended) The method according to claim 19, further comprising using a unique identifier associated with said at least one functional application ~~PSD~~ for retrieving said data or configuration changes.

26. (Currently Amended) The method according to claim 19, wherein at least one command or data executable by said at least one functional application is ~~issued~~ encrypted by said at least one HSM, routed through said communications pipe into said PSD, and processed by said at least one functional application.

27. (Previously Presented) The method according to claim 19 further comprising functionally connecting said local client and said first server through a private network.

28. (Previously Presented) The method according to claim 19 further comprising functionally connecting said local client and said first server through a public network.

29. (Previously Presented) The method according to claim 19 further comprising employing an asymmetric cryptographic component for said HSM cryptographic component and said PSD cryptographic component.

30. (Previously Presented) The method according to claim 19 further comprising employing a symmetric cryptographic component for said HSM cryptographic component and said PSD cryptographic component.

31. (Previously Presented) The method according to claim 19 further comprising using a secure communications protocol for said communications pipe.